FortiAnalyzer v5.0.7
Upgrade Guide

FortiAnalyzer v5.0.7 Upgrade Guide

June 27, 2014

05-507-245305-20140627

Fortinet Document Library	docs.fortinet.com
Fortinet Video Library	video.fortinet.com
Fortinet Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2014-06-27	Initial release.

FortiAnalyzer Firmware

This document provides an overview of FortiAnalyzer firmware and highlights general information you should be aware of prior to upgrading your FortiAnalyzer device. This guide is intended to supplement the *FortiAnalyzer Release Notes* documentation.

The following topics are included in this section:

- Best practices
- Firmware image naming convention
- FortiAnalyzer VM firmware
- SNMP MIB download
- Build numbers
- Firmware upgrade and support information

Best practices

Before any firmware upgrade complete the following:

- Download the FortiAnalyzer firmware image and Release Notes document from the Fortinet Customer Service & Support portal. Review the Release Notes including special notices, upgrade information, product integration and support, resolved and known issues.
- Prepare your FortiAnalyzer for upgrade and ensure your log devices are running the appropriate firmware versions as documented in the firmware Release Notes.
- Backup your configuration file and save this configuration file to your local computer. The device configuration file is saved with a `.dat` extension.

In VM environments, it is recommended that you clone the VM instance. In the event of an issue with the firmware upgrade, you can to revert to the VM clone.

In VM environments, upgrade your VM server to latest stable update and patch release offered by the VM host server provider.

- Plan a maintenance window to complete the firmware upgrade. If possible, you may want to set up a test environment to ensure that the upgrade does not negatively impact your network or log devices.
- Once the upgrade is complete, test your FortiAnalyzer device to ensure that the upgrade was successful and that all log devices are listed.

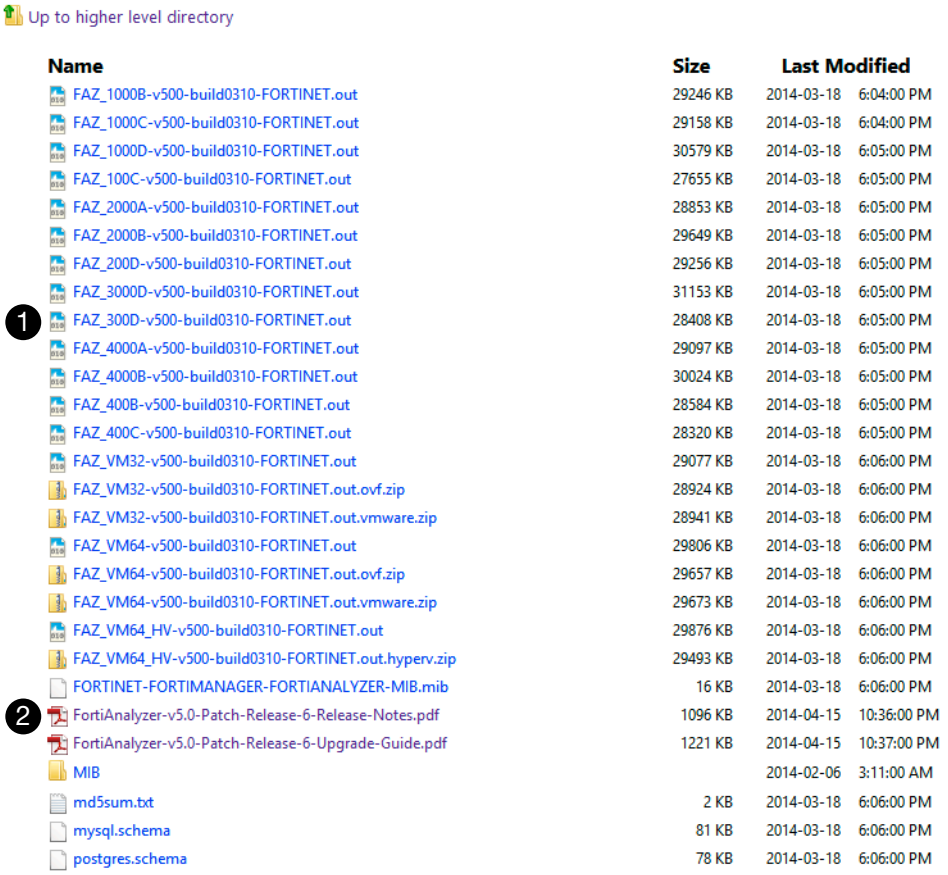
Firmware best practice: Stay current on patch releases for your current major release. Only upgrade to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the *FortiAnalyzer Release Notes* or contact Fortinet Technical Support.

Firmware image naming convention

FortiAnalyzer firmware images in the Fortinet Customer Service & Support portal HTTPS and FTP Download tabs are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the FAZ_300D-v500-build0310-FORTINET.out image found in the */FortiAnalyzer/v5.00/5.0/5.0.6* file folder is specific to the FortiAnalyzer 300D device model.

Figure 1 shows the */FortiAnalyzer/v5.00/5.0/5.0.6* file folder and highlights ❶ the firmware image for the FortiAnalyzer 300D and ❷ the location of the *FortiAnalyzer v5.0.6 Release Notes*.

Figure 1: v5.0.6 file folder



FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images for both VMware ESX/ESXi and Microsoft Hyper-V Server virtualization environments.

VMware ESX/ESXi

- FAZ_VMxx-v500-buildxxxx-FORTINET.out: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- FAZ_VMxx-v500-buildxxxx-FORTINET.out.ovf.zip: Download either the 32-bit or 64-bit package for new FortiAnalyzer VM installations. The package contains a deployable Open Virtualization Format (OVF) virtual machine package for VMware ESX/ESXi installations and the faz.vmdk and datadrive.vmdk virtual machine disk format files.

Microsoft Hyper-V Server

- FAZ_VM64_HV-v500-buildxxxx-FORTINET.out: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- FAZ_VM64_HV-v500-buildxxxx-FORTINET.out.hyperv.zip: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.

For more information see the FortiAnalyzer product data sheet available on the Fortinet web site, http://www.fortinet.com/products/fortianalyzer/virtualappliances.html.

SNMP MIB download

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiAnalyzer v5.00 file folder.

Build numbers

FortiAnalyzer firmware images are generally documented as a three-digit build number. New FortiAnalyzer models may be released on a special branch based off of the regular FortiAnalyzer firmware release. As such, the build number found in the *System Settings* > *Dashboard, System Information* widget and the output from the `get system status` CLI command displays this four-digit special build number as the build number.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a `Branch point:` field that displays the regular three-digit build number.

The following examples provide the output from the `get system status` CLI command for both a regular firmware release and a new model firmware release.

Example 1: Regular firmware release

```
Platform Type : FAZ2000A
Version : v5.0-build0232 130328 (GA Patch 4)
Serial Number : FLG-2K3F08000000
BIOS version : 04000001
Hostname : FortiAnalyzer-2000A
Max Number of Admin Domains : 2000
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
Branch Point : 232
```

```
Release Version Information : (GA Patch 4)
Current Time : Wed Sep 13 14:20:53 PDT 2013
Daylight Time Saving : Yes
Time Zone : (GMT-8:00)Pacific Time(US&Canada)

Disk Usage : Free 1825.27GB, Total 1831.40GB
RAID Level: Raid-5
RAID Status: OK
RAID Size: 1862GB

Disk 1: OK Used 465GB
Disk 2: OK Used 465GB
Disk 3: OK Used 465GB
Disk 4: OK Used 465GB
Disk 5: OK Not-Used 465GB
Disk 6: OK Used 465GB
```

Example 2: New model firmware release

```
Platform Type : FAZ300D
Version : v5.0-build4015 130416 (GA)
Serial Number : FL300D3M00000000
BIOS version : 00010001
System Part-Number : P13424-01
Hostname : FAZ300D
Max Number of Admin Domains : 175
Admin Domain Configuration : Disabled
FIPS Mode : Disabled
Branch Point : 151
Release Version Information : (GA)
Current Time : Tue Apr 23 15:09:43 PDT 2013
Daylight Time Saving : Yes
Time Zone : (GMT-8:00)Pacific Time(US&Canada)

Disk Usage : Free 1831.09GB, Total 1833.78GB
RAID Level: Raid-1
RAID Status: OK
RAID Size: 1953GB

Disk 1: OK Used 1953GB
Disk 2: OK Used 1953GB
```

Firmware upgrade and support information

The following table is for reference only. Review the applicable *FortiAnalyzer Releases Notes* prior to upgrading your FortiAnalyzer system.

The following table uses the naming convention '4.3.7', where the first digit reflects the version, the second digit reflects the major release, and the third digit reflects the patch release. For example, 4.3.7 is v4.0 MR3 Patch Release 7.

Table 1: FortiAnalyzer upgrade and support information

FortiAnalyzer Firmware Version	Build Number	Upgrade From	FortiOS Version Support
FortiAnalyzer 5.0			
5.0.7 Release Date: 2014-06-27	0321	5.0.6	5.2.0 5.0.0 to 5.0.7 4.3.2 or later 4.2.0 or later
FortiAnalyzer 5.0.7 is available for the following models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3500E, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.			
5.0.6 Release Date: 2014-02-05	0310	5.0.5 4.3.7 or later	5.0.0 to 5.0.7 4.3.2 or later 4.2.0 or later
FortiAnalyzer 5.0.6 is available for the following models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV. FAZ-3000E is released on special build 4047. FAZ-3500E is released on special build 4031.			
5.0.5 Release Date: 2013-11-08	0266	5.0.4 4.3.7	5.0.0 to 5.0.4 4.3.2 or later 4.2.0 or later
FortiAnalyzer 5.0.5 is available for the following models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.			
5.0.4 Release Date: 2013-09-13	0232	5.0.3	5.0.0 to 5.0.4 4.3.2 or later 4.2.0 or later
FortiAnalyzer 5.0.4 is available for the following models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV.			
5.0.3 Release Date: 2013-07-10	0200	5.0.1 or 5.0.2	5.0.0 to 5.0.3 4.3.2 or later 4.2.0 or later

Table 1: FortiAnalyzer upgrade and support information (continued)

FortiAnalyzer Firmware Version	Build Number	Upgrade From	FortiOS Version Support
FortiAnalyzer 5.0.3 is available for the following models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-4000A, FAZ-4000B, FAZ-VM32, FAZ-VM64, and FAZ-VM64-HV. FAZ-VM64-HV is released on the regular build. FAZ-1000D is released on special build 4024.			
5.0.2 Release Date: 2013-03-28	0151	5.0.1	5.0.0 to 5.0.2 4.3.2 or later 4.2.0 or later
FortiAnalyzer 5.0.2 is available for the following models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64. The FAZ-300D is released on special build 4018. The FAZ-3000D is released on special build 4014.			
5.0.1 Release Date: 2012-11-21	0087	4.3.5 or later	5.0.0 and 5.0.1 4.3.1 or later 4.2.0 or later
FortiAnalyzer 5.0.1 is available for the following models: FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64. The FAZ-300D is released on special build 4008.			
5.0.0 Release Date: 2012-11-01	0076	Note: This image was removed from the Customer Service & Support portal. For more information, see the *Customer Support Bulletin* in the image directory.	
FortiAnalyzer 4.3			
4.3.8 Release Date: 2013-11-26	0719	4.3.5 or later 4.2.6	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.8 is available for the following models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
4.3.7 Release Date: 2013-04-04	0705	4.3.5 or later 4.2.6	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.7 is available for the following models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
4.3.6 Release Date: 2012-12-05	0691	4.3.5 4.2.6	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.6 is available for the following models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			

Table 1: FortiAnalyzer upgrade and support information (continued)

FortiAnalyzer Firmware Version	Build Number	Upgrade From	FortiOS Version Support
4.3.5 Release Date: 2012-07-24	0680	4.3.3 or later 4.2.6	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.5 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64. Note: There is no image available for the FAZ-200D.			
4.3.4 Release Date: 2012-07-18	0679	4.3.3 4.2.6	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.4 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64. Note: There is no image available for the FAZ-200D.			
4.3.3 Release Date: 2012-05-15	0654	4.3.2 4.2.6	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.3 is available for the following models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64. The FAZ-200D is released on special build 4010.			
4.3.2 Release Date: 2012-03-19	0632	4.3.1 4.2.5 or later	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.2 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64. The FAZ-400C is released on special build 4006.			
4.3.1 Release Date: 2011-10-06	0552	4.3.0 4.2.4 or later	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.1 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, and FAZ-VM.			
4.3.0 Release Date: 2011-06-30	0513	4.2.4 or later	4.3.0 or later
FortiAnalyzer 4.3.0 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, and FAZ-4000B. Note: There is no image available for the FAZ-VM.			
FortiAnalyzer 4.2 is no longer supported (EOS) as of April 07, 2013.			

Upon upgrading to FortiAnalyzer v5.0 Patch Release 1 or later, the system automatically begins converting the v4.0 MR3 logs, and inserts them into the SQL database. An icon appears at the top right corner after login to the Web-based Manager next to the logout and help buttons. This pops-up a small window displaying the progress. The time required depends on the size of the database.

Upgrading a FortiAnalyzer VM device from v4.0 MR3 Patch 6 or later to v5.0 Patch Release 1 or later is supported. The old VM license is converted into the new VM stackable license model. New VM installations running v5.0 Patch Release 1 or later can be deployed with the `.ovf` (VMware ESX/ESXi) or `.vhd` (Microsoft Hyper-V) file and application of either an old v4.0 MR3 or new v5.0 license.

FortiGate, FortiCarrier, FortiMail, FortiWeb, and syslog devices are supported in FortiAnalyzer v5.0 Patch Release 7. Other devices are not yet supported in FortiAnalyzer v5.0. For more information, see the *FortiAnalyzer v5.0.7 Release Notes*.

Upgrade Information

This section explains how to properly upgrade to FortiAnalyzer v5.0.7. The following topics are included in this section:

- Upgrading from FortiAnalyzer v5.0.6 or earlier
- Firmware upgrade steps
- Distributed upgrades
- Downgrading to previous versions

Upgrading from FortiAnalyzer v5.0.6 or earlier

FortiAnalyzer v5.0.7 has re-sized the flash partition storing system firmware. In order to accommodate the re-sizing, you MUST upgrade to FortiAnalyzer v5.0.6 first. The secondary firmware and System Settings stored in the partition will be lost after upgrade. Please reconfigure System Settings as needed.

In VM environments, you will need to change the hard disk provisioned size to 513MB or more before powering on the FortiAnalyzer VM.

Upgrading your FortiAnalyzer 400B to v5.0.7 requires you to use an interim step. You MUST upgrade to the image named *FAZ_400B-v500-FORTINET_UpgradeThisBuildFirst.out* before upgrading to regular v5.0.7 image. The upgrade path looks like this:

v5.0.6 or earlier > FAZ_400B-v500-FORTINET_UpgradeThisBuildFirst.out > v5.0.7

Please upgrade your FortiAnalyzer 100C, 2000A, or 4000A via the Web-based Manager or command line interface. Upgrade via TFTP from BIOS is not supported for these models.

Firmware upgrade steps

The following table lists the firmware upgrade steps.

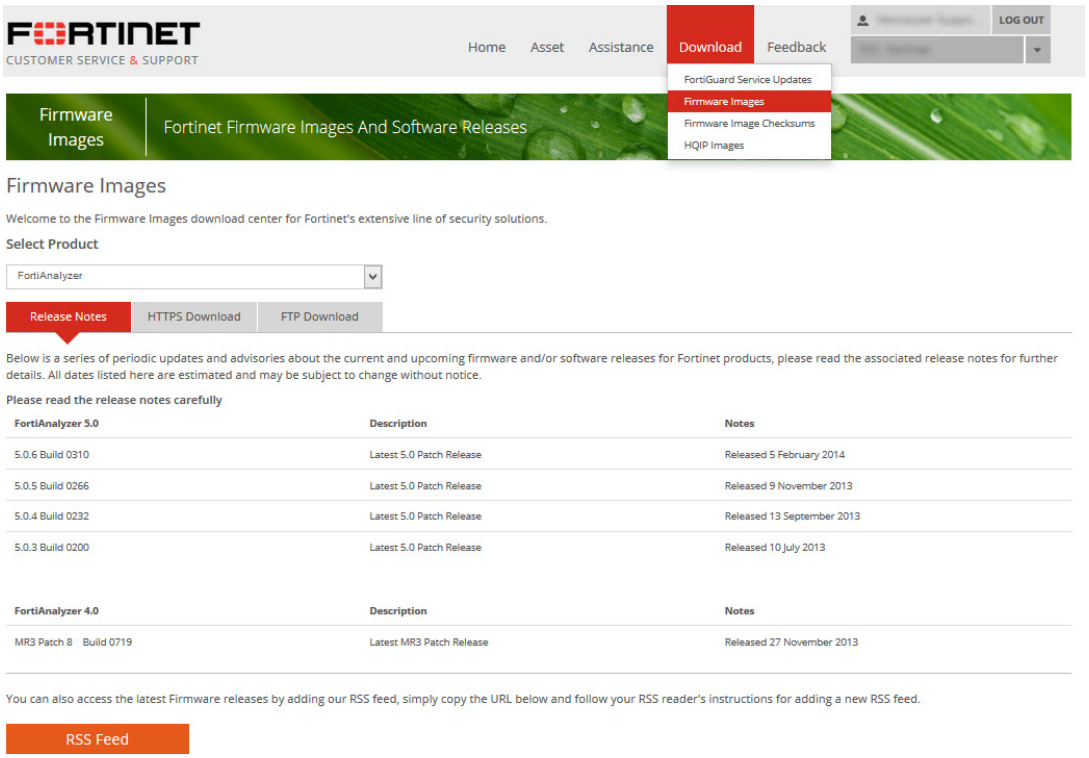
Table 2: Upgrade steps

Step 1	Prepare your FortiAnalyzer for upgrade.
Step 2	Backup your FortiAnalyzer system configuration. For FortiAnalyzer VM, clone the VM instance.
Step 3	For FortiAnalyzer VM, change the hard disk provisioned size.
Step 4	Transfer the firmware image to your FortiAnalyzer device.
Step 5	Log into your FortiAnalyzer Web-based Manager to verify the upgrade was successful.

Step 1: Prepare your FortiAnalyzer for upgrade

1. Make sure all log devices are running the supported firmware version as stated in the Release Notes.
2. Log in to the Fortinet Customer Service & Support portal at https://support.fortinet.com.
3. Select *Download* from the toolbar and select *Firmware Images* from the drop-down list.

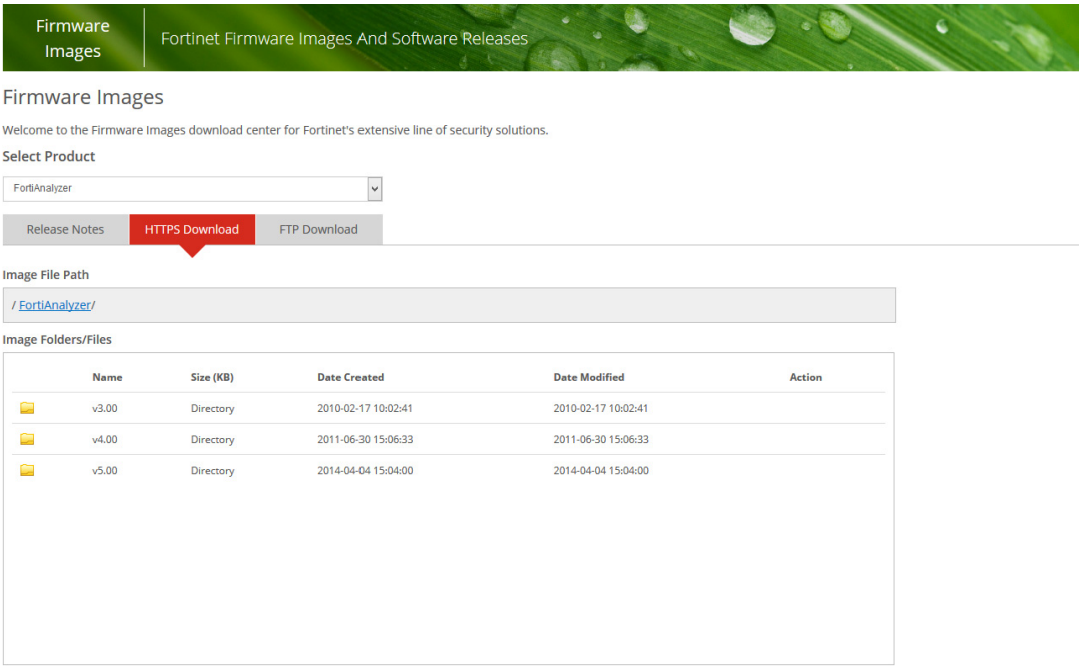
Figure 2: Firmware image page



4. Select *FortiAnalyzer* from the drop-down list and select the *HTTPS Download* tab. Alternatively, you can select *FTP Download*. FTP is not an encrypted file transferring protocol and HTTPS download is recommended.

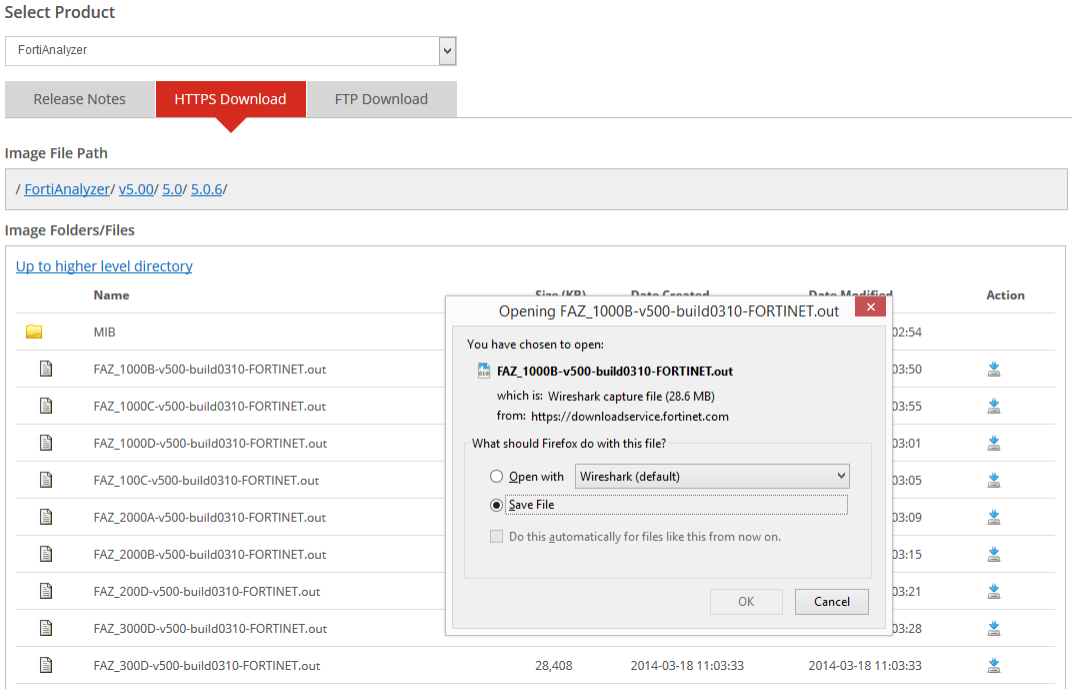
   The image folders are displayed.

Figure 3: Example image folders



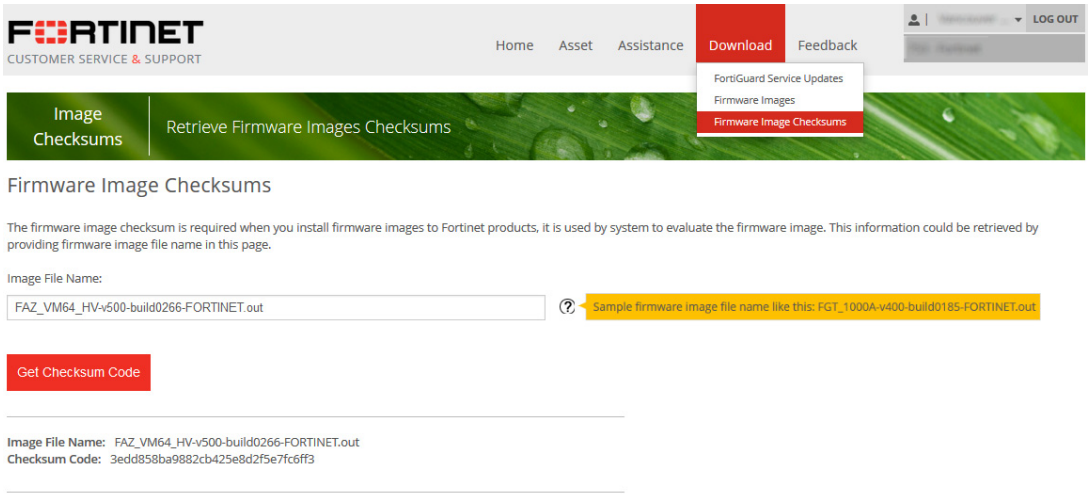
5. Browse to the appropriate file folder to download the firmware image (`.out`) and Release Notes document.

Figure 4: Download firmware image



6. Select an image in the list to download the firmware image to your management computer.
7. To verify the integrity of the download, select *Download* from the toolbar and select *Firmware Image Checksums* from the drop-down list.

Figure 5: Firmware image checksums page

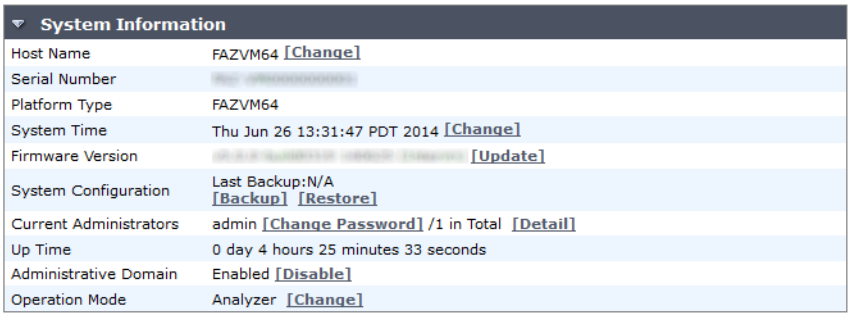


8. Enter the file name and select *Get Checksum Code* to get the firmware image checksum code. Compare this checksum with the checksum of the firmware image.

Step 2: Back up your FortiAnalyzer configuration

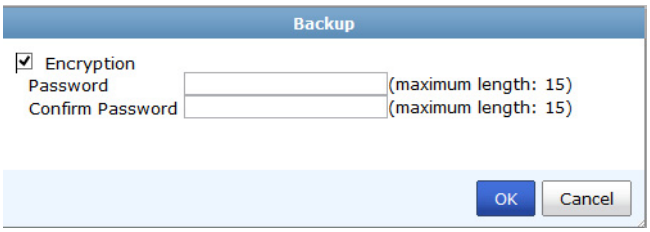
1. Go to *System Settings* > *Dashboard*.
2. Select *Backup* in the *System Information* widget.

Figure 6: System information widget



The *Backup* dialog box opens.

Figure 7: Backup dialog box



3. Select the checkbox to encrypt the backup file and enter a password.

When selecting to encrypt the backup configuration file, the same password used to encrypt the file will be required to restore this backup file to the FortiAnalyzer device.

4. Select *OK* and save the backup file on your local computer.

Optionally, you can backup the configuration file to a FTP, SFTP, or SCP server using the following CLI command:

```
execute backup all-settings {ftp | sftp} <server IP address>
    <path/filename to the server> <user name on server> <password>
    [cryptpasswd]
execute backup all-settings scp <server IP address> <path/filename to
    the server> <user name on server> <SSH certificate> <crptpassrd>
```

For more information, see the *FortiAnalyzer CLI Reference*.

5. In VM environments, it is recommended that you clone VM instance. In the event of an issue with the firmware upgrade, you can revert to the VM clone.

Step 3: Change the FortiAnalyzer VM hard disk provisioned size

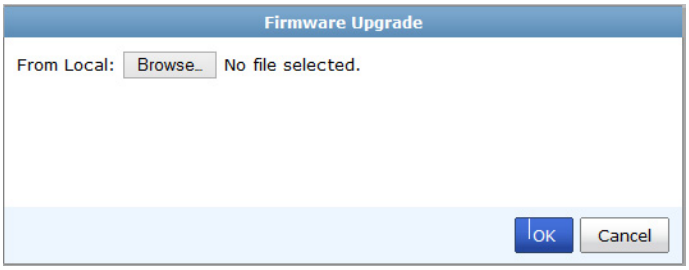
1. For VM environments, change the hard disk provisioned size to 513MB or more before upgrading your FortiAnalyzer VM.

Step 4: Transfer the firmware image to your FortiAnalyzer device

1. Go to *System Settings* > *Dashboard*.
2. In the *System Information* widget, in the *Firmware Version* field, select *Update*.

   The *Firmware Upgrade* dialog box opens.

Figure 8: Firmware upgrade dialog box



3. Select *Browse* to locate the firmware image (`.out` file) that you downloaded from the Fortinet Customer Service & Support portal and select *Open*.
4. Select *OK* to continue with the upgrade. *Your* FortiAnalyzer will upload the firmware image and you will receive a confirmation message noting that the upgrade was successful.

Optionally, you can upgrade firmware stored on a FTP or TFTP server using the following CLI command:

```
exexute restore image {ftp | tftp} <file path on the FTP server>
    <server IP address <user name on server> <password>
```

For more information, see the *FortiAnalyzer CLI Reference*.

Step 5: Verify the upgrade

1. Refresh the browser page and log back into the device.
2. Launch the *Device Manager* module and make sure that all formerly added log devices are still listed.
3. Launch the other functional modules and make sure they work properly.

Distributed upgrades

For Collector/Analyzer architecture upgrades, Fortinet recommends upgrading the Analyzer first.

Upgrading the Collector first could impact the Analyzer's performance.

Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous FortiAnalyzer firmware release via the Web-based Manager or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```